

UNITED STATES DISTRICT COURT

for the
Western District of Washington

FILED	LODGED
RECEIVED	
JAN 03 2020	
CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT TACOMA	
BY	DEPUTY

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 Subject Premises at 20205 117th Avenue East,
 Graham, Washington 98338 and Subject Person of
 NATHANIEL MARCUS SCOTT

Case No.

MJ20-5002

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The Subject Premises and Person as further described in Attachment A, attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18, U.S.C. § 2252 (a)(2)	Receipt or Distribution of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

- ☒ See attached Affidavit continued on the attached sheet

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

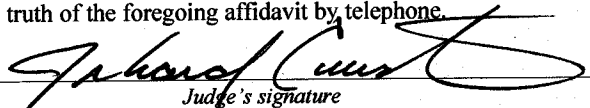
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means; or: ☐ telephonically recorded.


 Applicant's signature

Kelsey Mendoza, Special Agent FBI
 Printed name and title

- ☒ The foregoing affidavit was sworn to before me and signed in my presence, or
☐ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 01/03/2020


 Judge's signature

City and state: TACOMA, WASHINGTON

J. RICHARD CREATURA, U.S. MAGISTRATE JUDGE
 Printed name and title

ATTACHMENT A

Description of Property to be Searched

1. The physical address of the SUBJECT PREMISES is 20205 117th Ave East, Graham, Washington 98338. The SUBJECT PREMISES is further described as the property containing a single family, single story residence located in Pierce County, WA.



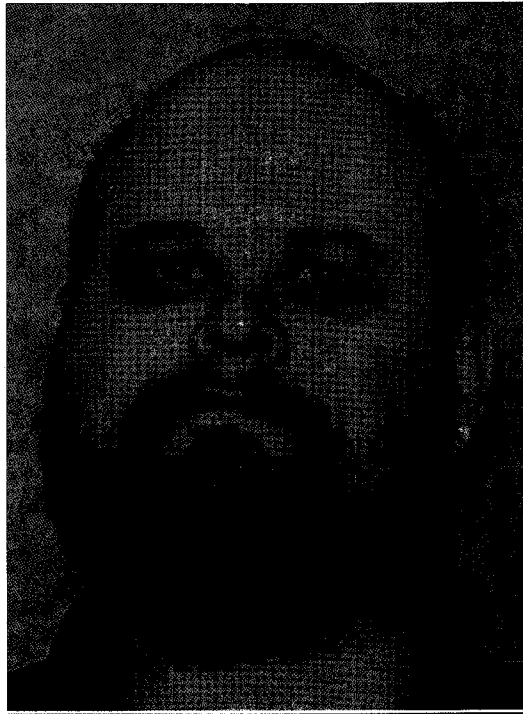
Back



The search is to include all rooms and vehicles on the SUBJECT PREMISES, as well as any garage/parking spaces or storage units/outbuildings located thereon and any digital device(s) found therein. Specifically, this warrant authorizes law enforcement to

1 seize and search any digital device law enforcement has probable cause to believe is
2 owned by or to which the SUBJECT PERSON has access. ~~For any other digital device,~~
3 ~~law enforcement may seize that device under this warrant but may not search it without~~
4 ~~approval from the Court.~~

5
6 The SUBJECT PERSON is NATHANIEL MARCUS SCOTT (DOB:
7 XX/XX/1973), pictured below:



ATTACHMENT B**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES or on the SUBJECT PERSON:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media and any items depicted in those visual depictions that may help to identify the person depicted or the creator of the depictions;

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence/records identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer, or evidences contact with minors;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

- 1 a. Any digital devices and storage device capable of being used to
2 commit, further, or store evidence of the offense listed above;
- 3 b. Any digital devices used to facilitate the transmission, creation,
4 display, encoding or storage of data, including word processing equipment, modems,
5 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;
- 6 c. Any magnetic, electronic, or optical storage device capable of
7 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
8 memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives,
9 camera memory cards, media cards, electronic notebooks, and personal digital assistants;
- 10 d. Any documentation, operating logs and reference manuals regarding
11 the operation of the digital device or software;
- 12 e. Any applications, utility programs, compilers, interpreters, and other
13 software used to facilitate direct or indirect communication with the computer hardware,
14 storage devices, or data to be searched;
- 15 f. Any physical keys, encryption devices, dongles and similar physical
16 items that are necessary to gain access to the computer equipment, storage devices or
17 data; and
- 18 g. Any passwords, password files, test keys, encryption codes or other
19 information necessary to access the computer equipment, storage devices or data;
- 20 8. Evidence of who used, owned or controlled any seized digital device(s) at
21 the time the things described in this warrant were created, edited, or deleted, such as logs,
22 registry entries, saved user names and passwords, documents, and browsing history;
- 23 9. Evidence of malware that would allow others to control any seized digital
24 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
25 as evidence of the presence or absence of security software designed to detect malware;
26 as well as evidence of the lack of such malware;
- 27 10. Evidence of the attachment to the digital device(s) of other storage devices
28 or similar containers for electronic evidence;

- 1 11. Evidence of counter-forensic programs (and associated data) that are
- 2 designed to eliminate data from a digital device;
- 3 12. Evidence of times the digital device(s) was used;
- 4 13. Any other ESI from the digital device(s) necessary to understand how the
- 5 digital device was used, the purpose of its use, who used it, and when.

6 14. Records and things evidencing the use of the IP addresses 73.221.4.33 (the
7 SUBJECT IP ADDRESS) including:

- 8 a. Routers, modems, and network equipment used to connect
- 9 computers to the Internet;
- 10 b. Records of Internet Protocol (IP) addresses used;
- 11 c. Records of Internet activity, including firewall logs, caches, browser
- 12 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
- 13 entered into any Internet search engine, and records of user-typed web addresses.

14 SEARCH TECHNIQUES

15 1. In this particular case, and in order to protect the third party privacy of
16 innocent individuals residing in the residence, the following are search techniques that
17 will be applied:

18 i. Device use and ownership will be determined through interviews, if
19 possible, and through the identification of user account(s), associated account names, and
20 log-ons associated with the device. Determination of whether a password is used to lock
21 a user's profile on the device(s) will assist in knowing who had access to the device or
22 whether the password prevented access.

23 ii. Use of hash value library searches.

24 iii. Use of keyword searches, i.e., utilizing key words that are known to be
25 associated with the sharing of child pornography.

26 iv. Identification of non-default programs that are commonly known to be used
27 for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent,
28 Ares, Shareaza, Gnutella, etc.

1 v. Looking for file names indicative of child pornography, such as, PTHC,
2 PTSC, Lolita, 3yo, etc. and file names identified during the undercover download of child
3 pornography.

4 vi. Viewing of image files and video files.

5 vii. As indicated above, the search will be limited to evidence of child
6 pornography and will not include looking for personal documents and files that are
7 unrelated to the crime.

8 2. These search techniques may not all be required or used in a particular
9 order for the identification of digital devices containing items set forth in Attachment B
10 to this Affidavit. However, these search techniques will be used systematically in an
11 effort to protect the privacy of third parties. Use of these tools will allow for the quick
12 identification of items authorized to be seized pursuant to Attachment B to this Affidavit,
13 and will also assist in the early exclusion of digital devices and/or files which do not fall
14 within the scope of items authorized to be seized pursuant to Attachment B to this
15 Affidavit.

16 3. In accordance with the information in this Affidavit, law enforcement
17 personnel will execute the search of digital devices seized pursuant to this warrant as
18 follows:

19 a. Upon securing the search site, the search team will conduct an initial
20 review of any digital devices/systems to determine whether the ESI contained therein can
21 be searched and/or duplicated on site in a reasonable amount of time and without
22 jeopardizing the ability to accurately preserve the data.

23 b. If, based on their training and experience, and the resources
24 available to them at the search site, the search team determines it is not practical to make
25 an on-site search, or to make an on-site copy of the ESI within a reasonable amount of
26 time and without jeopardizing the ability to accurately preserve the data, then the digital
27 devices will be seized and transported to an appropriate law enforcement laboratory for
28 review and to be forensically copied ("imaged"), as appropriate.

1 c. In order to examine the ESI in a forensically sound manner, law
2 enforcement personnel with appropriate expertise will produce a complete forensic
3 image, if possible and appropriate, of any digital device that is found to contain data or
4 items that fall within the scope of Attachment B of this Affidavit. In addition,
5 appropriately trained personnel may search for and attempt to recover deleted, hidden, or
6 encrypted data to determine whether the data fall within the list of items to be seized
7 pursuant to the warrant. In order to search fully for the items identified in the warrant,
8 law enforcement personnel, which may include investigative agents, may then examine
9 all of the data contained in the forensic image/s and/or on the digital devices to view their
10 precise contents and determine whether the data fall within the list of items to be seized
11 pursuant to the warrant.

12 d. The search techniques that will be used will be only those
13 methodologies, techniques and protocols as may reasonably be expected to find, identify,
14 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to
15 this Affidavit.

16 e. If, after conducting its examination, law enforcement personnel
17 determine that any digital device is an instrumentality of the criminal offenses referenced
18 above, the government may retain that device during the pendency of the case as
19 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
20 the chain of custody, and litigate the issue of forfeiture. If law enforcement determines
21 that a particular digital device was not an instrumentality of the offenses listed above, that
22 device shall be returned to the person from whom it was seized within sixty days of the
23 date of the warrant, unless the government seeks and obtains permission from the Court
24 for its retention.

25 4. In order to search for ESI that falls within the list of items to be seized
26 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and
27 search the following items (heretofore and hereinafter referred to as "digital devices"),
28 subject to the procedures set forth above:

1 a. Any digital device capable of being used to commit, further, or store
2 evidence of the offense(s) listed above;

3 b. Any digital device used to facilitate the transmission, creation,
4 display, encoding, or storage of data, including word processing equipment, modems,
5 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

6 c. Any magnetic, electronic, or optical storage device capable of
7 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
8 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
9 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

10 d. Any documentation, operating logs and reference manuals regarding
11 the operation of the digital device, or software;

12 e. Any applications, utility programs, compilers, interpreters, and other
13 software used to facilitate direct or indirect communication with the device hardware, or
14 ESI to be searched;

15 f. Any physical keys, encryption devices, dongles and similar physical
16 items that are necessary to gain access to the digital device, or ESI; and

17 g. Any passwords, password files, test keys, encryption codes or other
18 information necessary to access the digital device or ESI.

19 **The seizure of digital devices and/or their components as set forth herein is**
20 **specifically authorized by this search warrant, not only to the extent that such**
21 **digital devices constitute instrumentalities of the criminal activity described above,**
22 **but also for the purpose of the conducting off-site examinations of their contents for**
23 **evidence, instrumentalities, or fruits of the aforementioned crimes.**
24
25
26
27
28

1 **AFFIDAVIT**

2

3 STATE OF WASHINGTON,)

4) ss

5 COUNTY OF PIERCE)

6

7 I, Kelsey M. Mendoza, being duly sworn on oath, depose and state:

8 **I. INTRODUCTION AND AGENT BACKGROUND**

9 1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and

10 have been since January 2019. I am currently assigned to the Seattle Division's Tacoma

11 Resident Agency. As an FBI Special Agent, I investigate criminal violations relating to

12 child exploitation and child pornography, including violations pertaining to the illegal

13 production, distribution, receipt and possession of child pornography, and material

14 involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252,

15 2252A, 2422, and 2426. I have received specialized training from the FBI Academy

16 consisting of legal classes, investigative techniques, evidence preservation and collection,

17 financial related crimes, and other law enforcement training classes. During my

18 employment as a law enforcement officer, I have attended periodic seminars, meetings,

19 and continued training. Through my training and experience, I have developed an

20 understanding of common habits and practices used by those engaged in criminal acts

21 against children.

22 2. In preparing this affidavit, I have also consulted with Special Agent Kyle

23 McNeal, who has significant experience in the investigation of child exploitation

24 offenses, including both hands on sexual offenses involving children and the production

25 of trafficking in child pornography. SA McNeal has been an FBI special agent for over

26 eight years. As part of his duties, he investigates criminal violations relating to child

27 exploitation and child pornography, including violations pertaining to the illegal

28 production, distribution, receipt, and possession of child pornography and material

1 involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, and
2 2252A. He is a graduate of the FBI Academy and has received further specialized
3 training in investigating child pornography and child exploitation crimes. He has also
4 had the opportunity to observe and review examples of child pornography (as defined in
5 18 U.S.C. § 2256(8)). At this time, he is the South Sound Child Exploitation Task Force
6 (SSCETF) Coordinator and works with other federal, state, and local law enforcement
7 personnel in the investigation and prosecution of crimes involving the exploitation of
8 minors.

9 3. I make this Affidavit in support of an application under Rule 41 of the
10 Federal Rules of Criminal Procedure for a warrant to search the residence located at
11 20205 117th Avenue East, Graham, Washington 98338, (hereinafter the "SUBJECT
12 PREMISES") and the person of NATHANIEL MARCUS SCOTT (the "SUBJECT
13 PERSON"), as more fully described in Attachment A to this Affidavit, including any
14 digital devices, for the things described in Attachment B to this Affidavit, for evidence,
15 fruits, and instrumentalities of violations 18 U.S.C. § 2252(a)(2) (Receipt or Distribution
16 of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child
17 Pornography).

18 4. The facts set forth in this Affidavit are based on my own personal
19 knowledge; knowledge obtained from other individuals during my participation in this
20 investigation, including other law enforcement officers; review of documents and records
21 related to this investigation; communications with others who have personal knowledge
22 of the events and circumstances described herein; and information gained through my
23 training and experience.

24 5. Because this Affidavit is submitted for the limited purpose of establishing
25 probable cause in support of the application for a search warrant, it does not set forth
26 each and every fact that I or others have learned during the course of this investigation. I
27 have set forth only the facts that I believe are relevant to the determination of probable
28 cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §

1 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B)
2 (Possession of Child Pornography), will be found at the SUBJECT PREMISES or on the
3 SUBJECT PERSON.

4 II. STATEMENT OF PROBABLE CAUSE

5 6. On November 18, 2019, FBI Seattle received a lead from the FBI field
6 office in Washington, D.C., arising from a child pornography investigation into users of
7 Kik Messenger. Kik is a free mobile application that permits users to send text messages
8 and other content, including videos and images. Kik users can communicate with other
9 users one-on-one, or they can join chat groups and communicate with multiple users at
10 the same time. In either case, they can send and receive images, videos, and/or links to
11 such files. Kik is a commonly used platform for individuals who have an interest in the
12 sexual exploitation of children and child pornography to communicate about those copies
13 and share child exploitation imagery.

14 7. On or about August 5, 2019, an FBI online covert employee (OCE) entered
15 a private Kik group known to the OCE as a place where people meet, discuss, and trade
16 images of child pornography. Upon entering the group, the OCE saw an individual
17 known as FORGEIN TARGET¹, discussing his sexual interest in his 8-year old
18 daughter and send multiple pornographic and non-pornographic images purportedly of
19 her to the group. During a private conversation with FORGEIN TARGET through the
20 Kik application, the OCE received several additional child pornography images and
21 videos from that Kik user. An emergency disclosure request was sent to Kik for
22 subscriber identification information and IP access logs associated with the FORGEIN
23 TARGET.

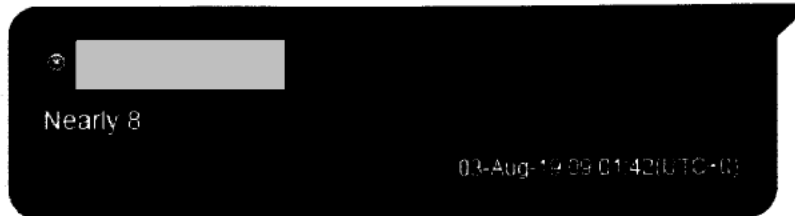
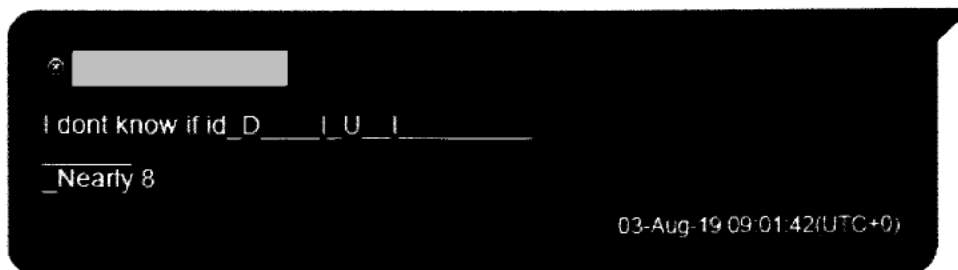
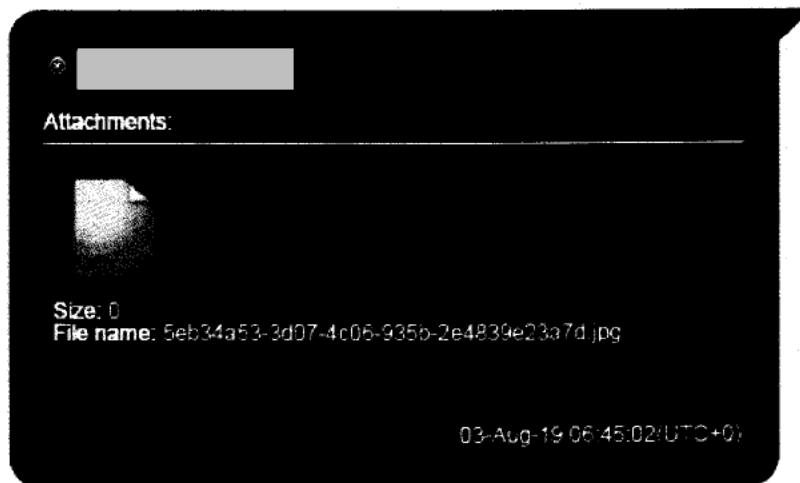
24
25
26
27 ¹ The online moniker of this offender is known to law enforcement, but I have not included it in this affidavit in
28 order to avoid public disclosure of information that could interfere with other investigation arising from FORGEIN
TARGET's arrest.

1 8. On or about August 7, 2019, law enforcement officers executed a search
2 warrant on the residence of FOREIGN TARGET, the Kik user described above, and
3 seized multiple devices used by FOREIGN TARGET to communicate on Kik. During a
4 forensic examination, law enforcement identified other Kik users with whom FOREIGN
5 TARGET communicated about child sexual abuse and child pornography, as well as logs
6 of their chats.

7 9. Among the Kik users who appears in these chat logs is user "ordoastrum."
8 Between August 3, and August 7, 2019, this user participated in a group chat that appears
9 to relate to the sexual exploitation of children and in which child exploitation material
10 was posted to that group. This user also discussed historic sexual abuse of a minor
11 relative and shared numerous files with the group, though many of those (which from
12 context appear likely to be child exploitation material) were not recovered. As detailed
13 below, further investigation revealed that the person using Kik account "ordoastum" is
14 the SUBJECT PERSON, who resides at the SUBJECT PREMISES.

15 10. Included below are examples of this group chat involving Kik user
16 "ordoastrum," the FOREIGN TARGET, and other Kik users. The chats were the result
17 of a forensic examination of the FOREIGN TARGET's phone upon arrest and were
18 provided to the FBI by a foreign law enforcement agency.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Here

03-Aug-19 09:26:32(UTC+0)



03-Aug-19 09:26:44(UTC+0)



ordoastrum Macgregor mathers

Well c'mon then. Lets go deliver.

03-Aug-19 17:04:55(UTC+0)



Lol yess how do we do this

03-Aug-19 17:05:35(UTC+0)



ordoastrum Macgregor mathers

Bring somebody comparable with and we double date .

03-Aug-19 17:13:29(UTC+0)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Omg

03-Aug-19 18:12:18(UTC+0)



She's special

03-Aug-19 18:12:24(UTC+0)



Same - mine loves Harry Potter

03-Aug-19 18:25:07(UTC+0)



Pm?

03-Aug-19 18:25:20(UTC+0)



Hi

03-Aug-19 22:56:42(UTC+0)



L Z has removed Admin from this group

03-Aug-19 23:03:19(UTC+0)



Wow

04-Aug-19 20:27:41(UTC+0)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Like?

04-Aug-19 20:29:54(UTC+0)



Attachments



Size: 0

File name: 9eaacf20fae652e768d6fa76a4f2e04d

04-Aug-19 20:31:46(UTC+0)



ordoastrum Macgregor mathers

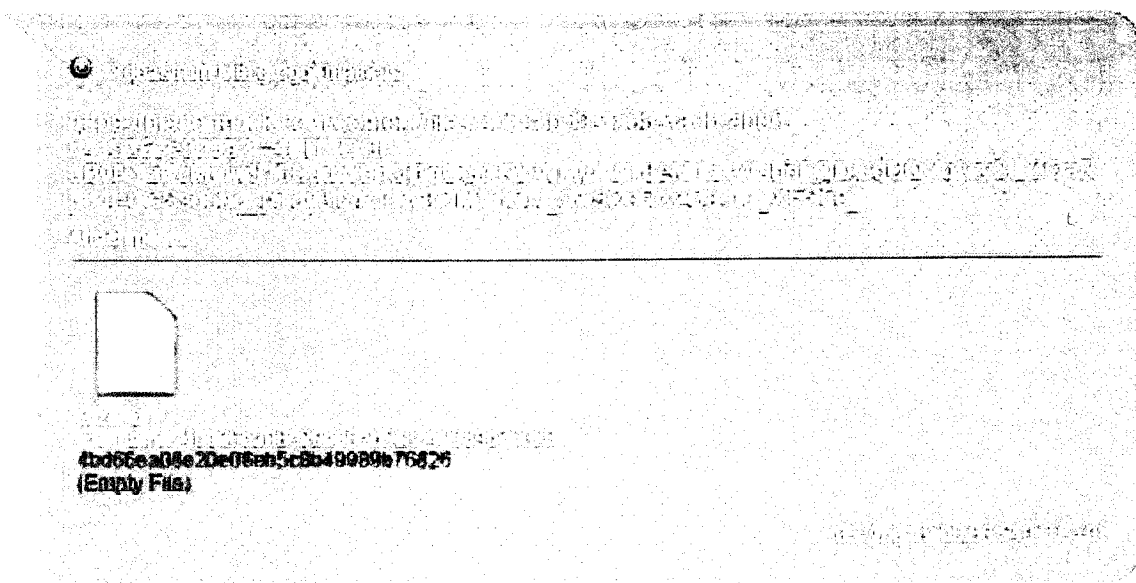
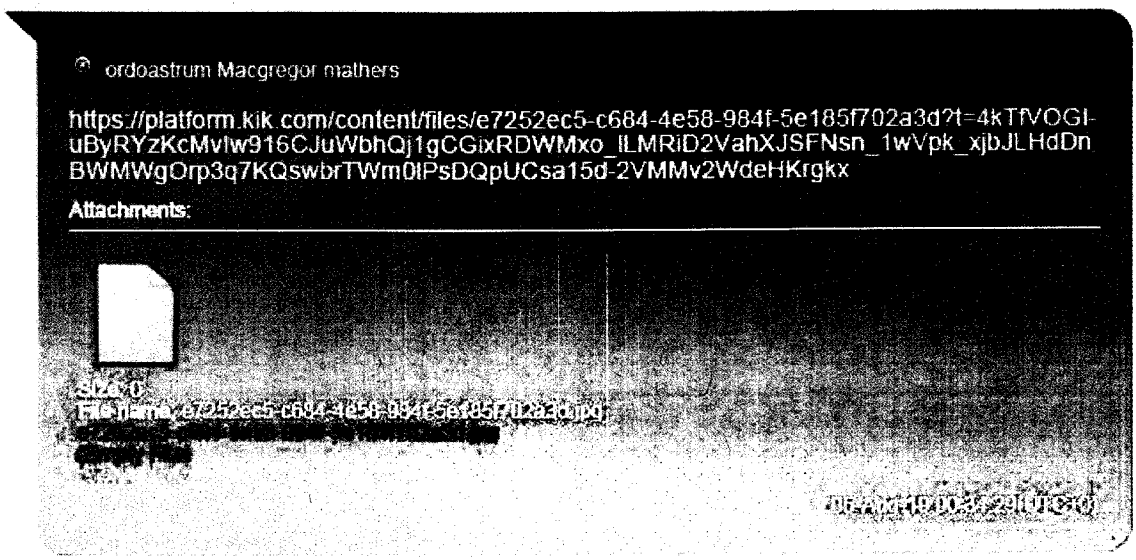
04-Aug-19 22:30:50(UTC+0)



ordoastrum Macgregor mathers

05-Aug-19 00:33:45(UTC+0)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[Redacted text]

[Redacted text]
<https://platform.kik.com/content/files/4a4ed0c3-dac9-4dde-8cd5-e4845a18e775?k=73a30f86972237311ae172a43c43d8772ccccGe6>
Attachments:
[Redacted text]
05-Aug-19 13:16:31(UTC+0)

[Redacted text]
What can I say... She loves doing handstands
05-Aug-19 13:17:15(UTC+0)

11. The image that has been redacted in the excerpt above (Image 1) shows a prepubescent female, with no visible pubic hair. She is nude and doing a handstand, and her genitals are exposed to the camera. Based on the chat conversation, the female is believed to be eight years old.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



It's going good.

05-Aug-19 13:24:52(UTC+0)



ordoastrum Macgregor mathers

Young women are great

05-Aug-19 14:39:53(UTC+0)



Wow! How do you survive

05-Aug-19 14:39:56(UTC+0)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



How old are yours?

05-Aug-19 19:55:06(UTC+0)



3 and 5

05-Aug-19 19:55:14(UTC+0)



ordoastrum Macgregor mathers

Oh well ya. I don't mean to say that any age isn't good. I was just saying that I like those two ages in particular

05-Aug-19 19:55:35(UTC+0)



We understand.

05-Aug-19 19:55:50(UTC+0)



We all have our favorites

05-Aug-19 19:56:43(UTC+0)



In my case if there's grass on the field play ball. Lolol

05-Aug-19 19:57:24(UTC+0)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

👤 ordoastrum Macgregor mathers

Hey lead, I believe the rest of that saying is " if there isn't, roll them over and play in the mud"

05-Aug-19 20:15:05(UTC+0)

👤 [REDACTED]

Hahahahaha. Yes

05-Aug-19 20:15:26(UTC+0)

👤 ordoastrum Macgregor mathers

She naked with daddy in the shower?

06-Aug-19 01:32:12(UTC+0)

👤 [REDACTED]

Well you Don t shower with clothes on.

06-Aug-19 01:32:59(UTC+0)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



3 is a great age - so curious and innocent

06-Aug-19 01:33:22(UTC+0)



ordoastrum Macgregor mathers

Lol. That is a truth. Just establishing a couple of facts. Makes the fantasy jerk off later more accurate


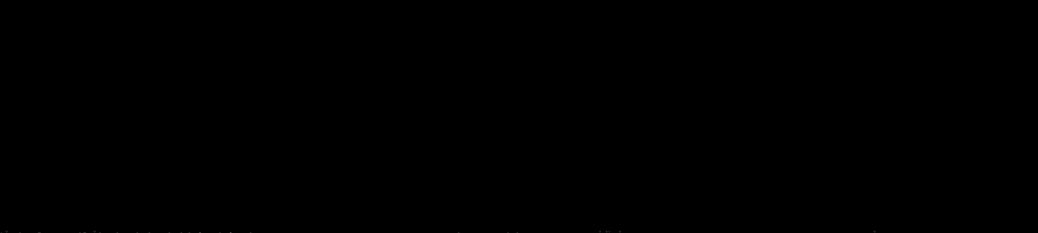
06-Aug-19 01:33:49(UTC+0)





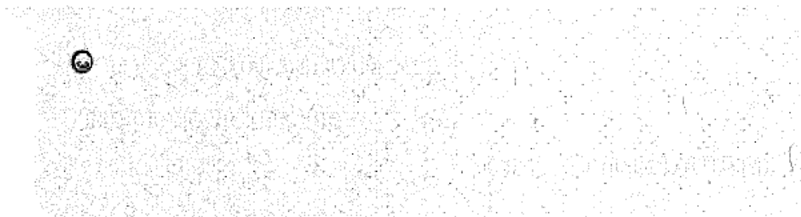
Willing to learn anything and everything

06-Aug-19 01:33:51(UTC+0)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

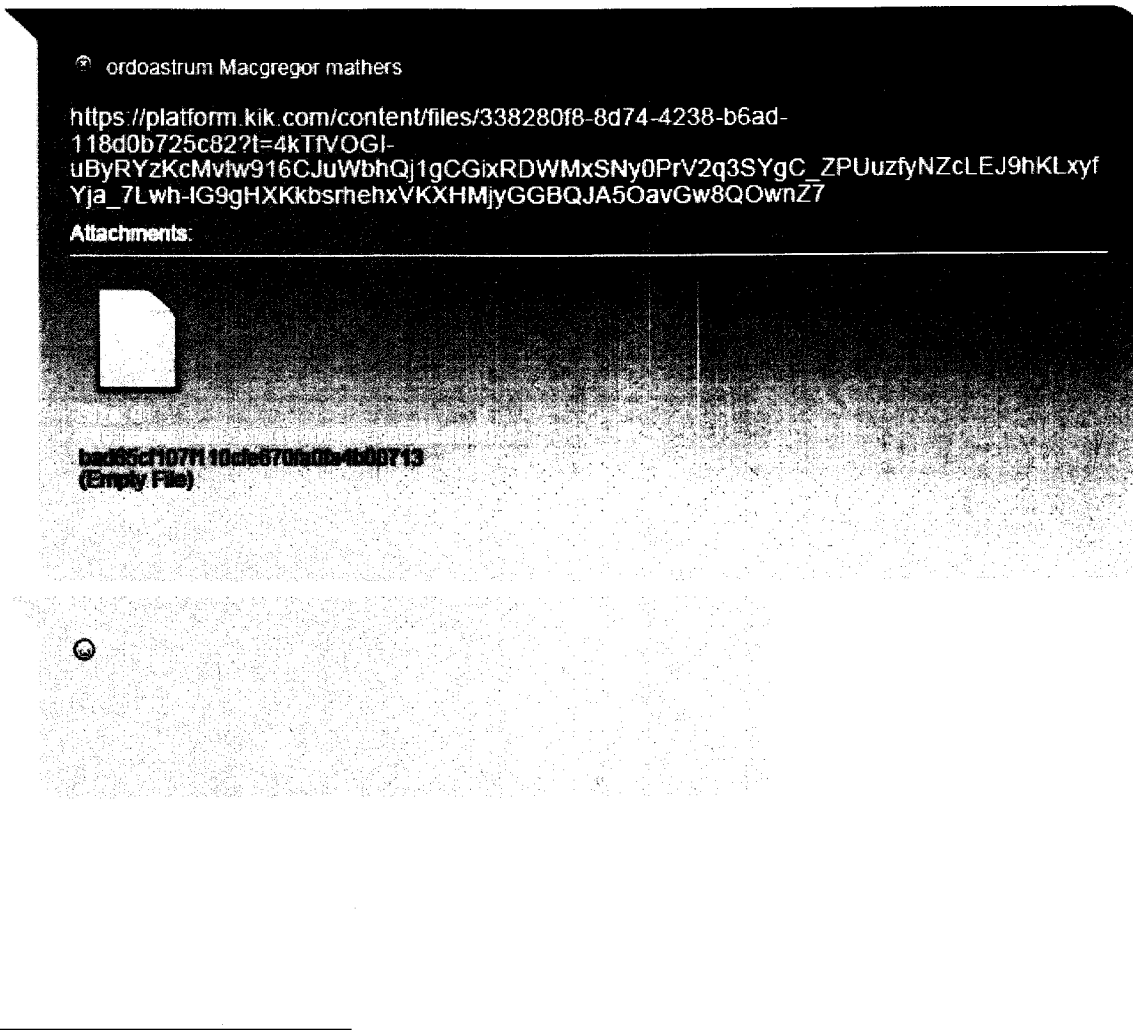

<https://platform.kik.com/content/files/b702c79f-e8b7-4aa8-8eef-3227c4636262?k=baa66cdd901b1e6d49e2ebd35f75e5039ecfe866>
Attachments:

06-Aug-19 11:09:45(UTC+0)


Bath time was fun though
06-Aug-19 11:09:57(UTC+0)


Almost 8
06-Aug-19 11:22:21(UTC+0)


12. The image that has been redacted in the excerpt above (Image 2²) shows a prepubescent female, with no visible pubic hair. She is naked, in a bath tub, and photographed from the waist down. Her legs are over the side of the bath tub with her genital area exposed to the camera while she is holding to the side of the tub. The FOREIGN TARGET stated the image was of his daughter, who was "almost 8".



² Copies of Image 1 and Image 2 will accompany this affidavit. A disc containing these files will be made available to the reviewing magistrate as part of the presentation of this search application and placed in an envelope marked Exhibit 1. Exhibit 1 will be provided to the reviewing magistrate judge as part of this search application but will not be filed with the Court. Exhibit 1 will remain in the custody of the FBI to be made available should it be relevant to any future legal proceedings related to the execution of the search.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28


Fuck... that got me up
06-Aug-19 13:52:29(UTC-0)

 ordoastrum Macgregor mathers
She is bushy. I like that.
06-Aug-19 14:15:27(UTC+0)

ordoastrum Macgregor mathers

https://platform.kik.com/content/files/8a6eb018-226d-4d1b-ace5-8b79047e8370?l=4kTrVOGI-uByRYzKcMvIw916CJuWbhQj1gCGixRDWMxKyd9kvHHDY_jqmc3kFEM0a-YRlu7K-ZpxB1QdGsEESojXThwE-bXmDsotUpxFi-kDFYxw6NMHp1balhLTa

Attachments:



h420467ab991ddb402b555em31531c
(Empty File)

ordoastrum Macgregor mathers

https://platform.kik.com/content/files/8a6eb018-226d-4d1b-ace5-8b79047e8370?l=4kTrVOGI-uByRYzKcMvIw916CJuWbhQj1gCGixRDWMxKyd9kvHHDY_jqmc3kFEM0a-YRlu7K-ZpxB1QdGsEESojXThwE-bXmDsotUpxFi-kDFYxw6NMHp1balhLTa

Attachments:



h420467ab991ddb402b555em31531c
(Empty File)

Admin has left the chat

06-Aug-19 14:50:06(UTC+0)

ordoastrum Macgregor mathers

What is going on here? Show some pussy and folks bail?

06-Aug-19 15:07:40(UTC+0)

dcjohn1996 John P

https://platform.kik.com/content/files/a895fe76-7d25-4aea-926e-c0a14c90530d?t=4kTfVOGI-uByRYzKcMvIw916CJuWbhQj1gCGixRDWMzUdvcHfBxkTmlUVi-mC9nL7-OyYuVAm1dbTTYbw5dMutsa7giKnFeyVihjc5_e9-sa15d-2VMMv2WdeHlKrgkx


Attachments:

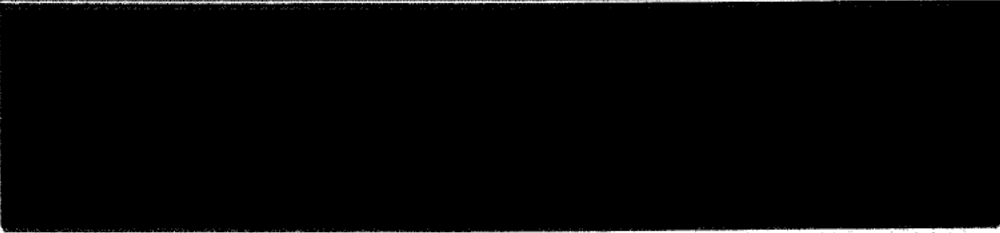


SA MENDOZA AFFIDAVIT - 19
USAO #2019R01264


UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28


Need to wait till she falls asleep
06-Aug-19 15:13:50(UTC+0)

ordoastrum Macgregor mathers
https://platform.kik.com/content/files/a0c11808-c985-4f6d-bb83-a0b11a739165?t=4kTfVOGI-uByRYzKcMvIw916CJuWbhQj1gCG6xRDWMxB8_CsTadm0yIRVsjd28s0oXySU76vqW-14t0CxHg1aTn8CYhwWCmssqdrclUVF_9w5QsRzOa-1a_XFS5e_
Attachments:


13. The image above, which has been redacted, shows a male penis and a pair of purple underwear with ejaculate on them.

ordoastrum Macgregor mathers

06-Aug-19 17:14:46(UTC+0)

1
2 ordoastrum Macgregor mathers

3
4 06-Aug-19 20:58:09(UTC+0)

5
6
7
8 06-Aug-19 21:08:26(UTC+0)

9
10 ordoastrum Macgregor mathers

11
12 06-Aug-19 21:51:53(UTC+0)

13
14 ordoastrum Macgregor mathers

15 Have always thought so. Although you fellas got some real pretty girls yerselves.

16 06-Aug-19 22:38:07(UTC+0)

1
2
3 13

4 06-Aug-19 22:46:51(UTC+0)

5
6 ordoastrum Macgregor mathers

7 God I love her. I would pay just to see her O face

8 06-Aug-19 22:47:42(UTC+0)

9
10 ordoastrum Macgregor mathers

11 Well see her make her O face

12 06-Aug-19 22:48:00(UTC+0)

13
14
15 It's awesome

16 06-Aug-19 22:48:32(UTC+0)

17
18 ordoastrum Macgregor mathers

19 Lead pm?

20 06-Aug-19 22:49:28(UTC+0)

21
22 14. In response to an administrative subpoena, Kik provided the following
23 subscriber information for user ordoastrum.

24 Username: Ordoastrum

25 Display Name: Macgregor mathers

26 Email: samaelfff@hotmail.com

27 Device: LGE android LM-Q710(FGN)

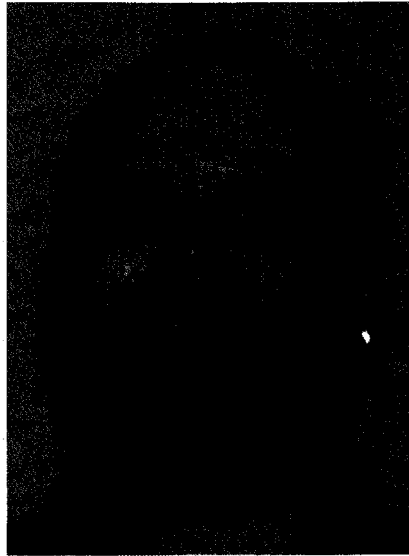
1 15. Included in the kik response were IP access logs spanning August 14, 2019,
2 through September 13, 2019. Examination of the logs showed Kik user "ordoastrum"
3 used IP addresses belonging to Comcast Communication and T-Mobile to access Kik
4 during this period. Among these was Comcast IP address 73.221.4.33 (the SUBJECT IP
5 ADDRESS).

6 16. In response to an administrative subpoena, Comcast reported that the
7 SUBJECT IP ADDRESS was assigned to Kerstin Scott with a service address at the
8 SUBJECT PREMESIS on August 14, 2019, with a lease grant date of March 21, 2019,
9 and a lease expiration of September 16, 2019.

10 17. Open source searches for the email address samuelfff@hotmail.com (the
11 email address linked to Kik user "ordoastrum") revealed other social media accounts
12 linked to that email address, including Twitter (username: samaelfff; display name:
13 Nathaniel), LinkedIn (name: nathaniel scott), and Skype (username: samaelfff; display
14 name: nathaniel scott).

15 18. On November 21, 2019, Kimberly Myhrer, a U.S. Postal Inspector,
16 confirmed that four individuals received mail at the SUBJECT PREMISES: Nathaniel
17 Scott, Kerstin Scott, and their two minor children.

18 19. Department of Licensing (DOL) information was requested for SUBJECT
19 PERSON. The following DOL image was provided for that individual. DOL records
20 also show SUBJECT PERSON lists his residence as 20205 117th East, Graham, WA
21 98338, the SUBJECT PREMISES.



20. As noted above, the chat logs involving Kik user “ordoastrum” cover the period between August 3, and August 7, 2019. However, the records available from Kik show only that the SUBJECT IP ADDRESS was used by “ordoastrum” to connect to Kik between August 14, 2019 and September 13, 2019. I know from my training and experience that Kik users rarely, if ever, share Kik accounts. That is, once a Kik account is created, the same person who created it will continue to use it. I also know that whenever a Kik user logs in to Kik on a mobile device with their username and password, any stored content associated with that account on other mobile devices is deleted. As such, Kik users generally use one device to access their account at a time. The fact that Kik user “ordoastrum” accessed Kik from multiple IP addresses, including IP addresses assigned to Comcast and T-Mobile, suggests, as is common for Kik users, that he used the same mobile device to access this account from various locations. I therefore believe it is likely that the person who connected to Kik using the SUBJECT IP ADDRESS is the same person who participated in the Kik chat described above.

III. TECHNICAL BACKGROUND

21. Based on my training and experience, when an individual communicates through the Internet, the individual leaves an IP address which identifies the individual

1 user by account and ISP (as described above). When an individual is using the Internet,
2 the individual's IP address is visible to administrators of websites they visit. Further, the
3 individual's IP address is broadcast during most Internet file and information exchanges
4 that occur.

5 22. Based on my training and experience, I know that most ISPs provide only
6 one IP address for each residential subscription. I also know that individuals often use
7 multiple digital devices within their home to access the Internet, including desktop and
8 laptop computers, tablets, and mobile phones. A device called a router is used to connect
9 multiple digital devices to the Internet via the public IP address assigned (to the
10 subscriber) by the ISP. A wireless router performs the functions of a router but also
11 includes the functions of a wireless access point, allowing (wireless equipped) digital
12 devices to connect to the Internet via radio waves, not cables. Based on my training and
13 experience, today many residential Internet customers use a wireless router to create a
14 computer network within their homes where users can simultaneously access the Internet
15 (with the same public IP address) with multiple digital devices.

16 23. Based on my training and experience and information provided to me by
17 computer forensic agents, I know that data can quickly and easily be transferred from one
18 digital device to another digital device. Data can be transferred from computers or other
19 digital devices to internal and/or external hard drives, tablets, mobile phones, and other
20 mobile devices via a USB cable or other wired connection. Data can also be transferred
21 between computers and digital devices by copying data to small, portable data storage
22 devices including USB (often referred to as "thumb") drives, memory cards (Compact
23 Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

24 24. As outlined above, residential Internet users can simultaneously access
25 the Internet in their homes with multiple digital devices. Also explained above is how
26 data can quickly and easily be transferred from one digital device to another through the
27 use of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage
28 devices (USB drives, memory cards, optical discs). Therefore, a user could access the

1 Internet using their assigned public IP address, receive, transfer or download data, and
2 then transfer that data to other digital devices, which may or may not have been
3 connected to the Internet during the date and time of the specified transaction.

4 25. Based on my training and experience, I have learned that the computer's
5 ability to store images and videos in digital form makes the computer itself an ideal
6 repository for child pornography. The size of hard drives used in computers (and other
7 digital devices) has grown tremendously within the last several years. Hard drives with
8 the capacity of four (4) terabytes (TB) are not uncommon. These drives can store
9 thousands of images and videos at very high resolution.

10 26. Based on my training and experience, and information provided to me by
11 other law enforcement officers, I know that people tend to use the same user names
12 across multiple accounts and email services.

13 27. Based on my training and experience, collectors and distributors of child
14 pornography also use online resources to retrieve and store child pornography, including
15 services offered by companies such as Google, Yahoo, Apple, and Dropbox, among
16 others. The online services allow a user to set up an account with a remote computing
17 service that provides email services and/or electronic storage of computer files in any
18 variety of formats. A user can set up an online storage account from any computer with
19 access to the Internet. Evidence of such online storage of child pornography is often
20 found on the user's computer. Even in cases where online storage is used, however,
21 evidence of child pornography can be found on the user's computer in most cases.

22 28. As is the case with most digital technology, communications by way of
23 computer can be saved or stored on the computer used for these purposes. Storing this
24 information can be intentional, i.e., by saving an email as a file on the computer or saving
25 the location of one's favorite websites in, for example, "bookmarked" files. Digital
26 information can also be retained unintentionally, e.g., traces of the path of an electronic
27 communication may be automatically stored in many places (e.g., temporary files or ISP
28 client software, among others). In addition to electronic communications, a computer

1 user's Internet activities generally leave traces or "footprints" and history files of the
2 browser application used. A forensic examiner often can recover evidence suggesting
3 whether a computer contains wireless software, and when certain files under investigation
4 were uploaded or downloaded. Such information is often maintained indefinitely until
5 overwritten by other data.

6 29. Based on my training and experience, I have learned that producers of
7 child pornography can produce image and video digital files from the average digital
8 camera, mobile phone, or tablet. These files can then be easily transferred from the
9 mobile device to a computer or other digital device, using the various methods described
10 above. The digital files can then be stored, manipulated, transferred, or printed directly
11 from a computer or other digital device. Digital files can also be edited in ways similar to
12 those by which a photograph may be altered; they can be lightened, darkened, cropped, or
13 otherwise manipulated. As a result of this technology, it is relatively inexpensive and
14 technically easy to produce, store, and distribute child pornography. In addition, there is
15 an added benefit to the child pornographer in that this method of production is a difficult
16 trail for law enforcement to follow.

17 30. As part of my training and experience, I have become familiar with the
18 structure of the Internet, and I know that connections between computers on the Internet
19 routinely cross state and international borders, even when the computers communicating
20 with each other are in the same state. Individuals and entities use the Internet to gain
21 access to a wide variety of information; to send information to, and receive information
22 from, other individuals; to conduct commercial transactions; and to communicate via
23 email.

24 31. Based on my training and experience, I know that cellular mobile phones
25 (often referred to as "smart phones") have the capability to access the Internet and store
26 information, such as images and videos. As a result, an individual using a smart phone
27 can send, receive, and store files, including child pornography, without accessing a
28 personal computer or laptop. An individual using a smart phone can also easily connect

1 the device to a computer or other digital device, via a USB or similar cable, and transfer
2 data files from one digital device to another. Moreover, many media storage devices,
3 including smartphones and thumb drives, can easily be concealed and carried on an
4 individual's person and smartphones and/or mobile phones are also often carried on an
5 individual's person.

6 32. As set forth herein and in Attachment B to this Affidavit, I seek
7 permission to search for and seize evidence, fruits, and instrumentalities of the above-
8 referenced crimes that might be found at the SUBJECT PREMISES or on the SUBJECT
9 PERSON, in whatever form they are found. It has been my experience that individuals
10 involved in child pornography often prefer to store images of child pornography in
11 electronic form. The ability to store images of child pornography in electronic form
12 makes digital devices, examples of which are enumerated in Attachment B to this
13 Affidavit, an ideal repository for child pornography because the images can be easily sent
14 or received over the Internet. As a result, one form in which these items may be found is
15 as electronic evidence stored on a digital device.

16 33. Based upon my knowledge, experience, and training in child
17 pornography investigations, and the training and experience of other law enforcement
18 officers with whom I have had discussions, I know that there are certain characteristics
19 common to individuals who have a sexualized interest in children and depictions of
20 children:

21 a. They may receive sexual gratification, stimulation, and satisfaction
22 from contact with children; or from fantasies they may have viewing children engaged in
23 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
24 visual media; or from literature describing such activity.

25 b. They may collect sexually explicit or suggestive materials in a
26 variety of media, including photographs, magazines, motion pictures, videotapes, books,
27 slides, and/or drawings or other visual media. Such individuals often times use these
28 materials for their own sexual arousal and gratification. Further, they may use these

1 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
2 selected child partner, or to demonstrate the desired sexual acts. These individuals may
3 keep records, to include names, contact information, and/or dates of these interactions, of
4 the children they have attempted to seduce, arouse, or with whom they have engaged in
5 the desired sexual acts.

6 c. They often maintain any "hard copies" of child pornographic
7 material that is, their pictures, films, video tapes, magazines, negatives, photographs,
8 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of
9 their home or some other secure location. These individuals typically retain these "hard
10 copies" of child pornographic material for many years, as they are highly valued.

11 d. Likewise, they often maintain their child pornography collections
12 that are in a digital or electronic format in a safe, secure and private environment, such as
13 a computer and surrounding area. These collections are often maintained for several
14 years and are kept close by, often at the individual's residence or some otherwise easily
15 accessible location, to enable the owner to view the collection, which is valued highly.

16 e. They also may correspond with and/or meet others to share
17 information and materials; rarely destroy correspondence from other child pornography
18 distributors/collectors; conceal such correspondence as they do their sexually explicit
19 material; and often maintain lists of names, addresses, and telephone numbers of
20 individuals with whom they have been in contact and who share the same interests in
21 child pornography.

22 f. They generally prefer not to be without their child pornography for
23 any prolonged time period. This behavior has been documented by law enforcement
24 officers involved in the investigation of child pornography throughout the world.

25 g. E-mail itself provides a convenient means by which individuals can
26 access a collection of child pornography from any computer, at any location with Internet
27 access. Such individuals therefore do not need to physically carry their collections with
28 them but rather can access them electronically. Furthermore, these collections can be

1 stored on email "cloud" servers, which allow users to store a large amount of material at
2 no cost, without leaving any physical evidence on the users' computer(s).

3 34. In addition to offenders who collect and store child pornography, law
4 enforcement has encountered offenders who obtain child pornography from the internet,
5 view the contents and subsequently delete the contraband, often after engaging in self-
6 gratification. In light of technological advancements, increasing Internet speeds and
7 worldwide availability of child sexual exploitative material, this phenomenon offers the
8 offender a sense of decreasing risk of being identified and/or apprehended with quantities
9 of contraband. This type of consumer is commonly referred to as a 'seek and delete'
10 offender, knowing that the same or different contraband satisfying their interests remain
11 easily discoverable and accessible online for future viewing and self-gratification. I
12 know that, regardless of whether a person discards or collects child pornography he/she
13 accesses for purposes of viewing and sexual gratification, evidence of such activity is
14 likely to be found on computers and related digital devices, including storage media, used
15 by the person. This evidence may include the files themselves, logs of account access
16 events, contact lists of others engaged in trafficking of child pornography, backup files,
17 and other electronic artifacts that may be forensically recoverable.

18 35. Given the above-stated facts, and based on my knowledge, training and
19 experience, along with my discussions with other law enforcement officers who
20 investigate child exploitation crimes, I believe that the SUBJECT PERSON is Kik user
21 "ordoastrum" and likely has a sexualized interest in children and depictions of children,
22 and that evidence of child pornography is likely to be found on digital media devices,
23 including mobile and/or portable digital devices that belong to this user or to which this
24 user has access.

25 36. Based on my training and experience, and that of computer forensic
26 agents that I work and collaborate with on a daily basis, I know that every type and kind
27 of information, data, record, sound or image can exist and be present as electronically
28 stored information on any of a variety of computers, computer systems, digital devices,

1 and other electronic storage media. I also know that electronic evidence can be moved
2 easily from one digital device to another. As a result, I believe that electronic evidence
3 may be stored on any digital device present at the SUBJECT PREMISES or on the
4 SUBJECT PERSON.

5 37. Based on my training and experience, and my consultation with
6 computer forensic agents who are familiar with searches of computers, I know that in
7 some cases the items set forth in Attachment B may take the form of files, documents,
8 and other data that is user-generated and found on a digital device. In other cases, these
9 items may take the form of other types of data - including in some cases data generated
10 automatically by the devices themselves.

11 38. Based on my training and experience, and my consultation with
12 computer forensic agents who are familiar with searches of computers, I believe that if
13 digital devices are found in the SUBJECT PREMISES or on the SUBJECT PERSON,
14 there is probable cause to believe that the items set forth in Attachment B will be stored
15 in those digital devices for a number of reasons, including but not limited to the
16 following:

17 a. Once created, electronically stored information (ESI) can be stored
18 for years in very little space and at little or no cost. A great deal of ESI is created, and
19 stored, moreover, even without a conscious act on the part of the device operator. For
20 example, files that have been viewed via the Internet are sometimes automatically
21 downloaded into a temporary Internet directory or "cache," without the knowledge of the
22 device user. The browser often maintains a fixed amount of hard drive space devoted to
23 these files, and the files are only overwritten as they are replaced with more recently
24 viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may
25 include relevant and significant evidence regarding criminal activities, but also, and just
26 as importantly, may include evidence of the identity of the device user, and when and
27 how the device was used. Most often, some affirmative action is necessary to delete ESI.

28

1 And even when such action has been deliberately taken, ESI can often be recovered,
2 months or even years later, using forensic tools.

3 b. Wholly apart from data created directly (or indirectly) by user-
4 generated files, digital devices - in particular, a computer's internal hard drive - contain
5 electronic evidence of how a digital device has been used, what it has been used for, and
6 who has used it. This evidence can take the form of operating system configurations,
7 artifacts from operating systems or application operations, file system data structures, and
8 virtual memory "swap" or paging files. Computer users typically do not erase or delete
9 this evidence, because special software is typically required for that task. However, it is
10 technically possible for a user to use such specialized software to delete this type of
11 information - and, the use of such special software may itself result in ESI that is relevant
12 to the criminal investigation. In particular, to properly retrieve and analyze electronically
13 stored (computer) data, and to ensure accuracy and completeness of such data and to
14 prevent loss of the data either from accidental or programmed destruction, it is necessary
15 to conduct a forensic examination of the computers. To effect such accuracy and
16 completeness, it may also be necessary to analyze not only data storage devices, but also
17 peripheral devices which may be interdependent, the software to operate them, and
18 related instruction manuals containing directions concerning operation of the computer
19 and software.

20 **V. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES**

21 39. In addition, based on my training and experience and that of computer
22 forensic agents that I work and collaborate with on a daily basis, I know that in most
23 cases it is impossible to successfully conduct a complete, accurate, and reliable search for
24 electronic evidence stored on a digital device during the physical search of a search site
25 for a number of reasons, including but not limited to the following:

26 a. Technical Requirements: Searching digital devices for criminal
27 evidence is a highly technical process requiring specific expertise and a properly
28 controlled environment. The vast array of digital hardware and software available

1 requires even digital experts to specialize in particular systems and applications, so it is
2 difficult to know before a search which expert is qualified to analyze the particular
3 system(s) and electronic evidence found at a search site. As a result, it is not always
4 possible to bring to the search site all of the necessary personnel, technical manuals, and
5 specialized equipment to conduct a thorough search of every possible digital
6 device/system present. In addition, electronic evidence search protocols are exacting
7 scientific procedures designed to protect the integrity of the evidence and to recover even
8 hidden, erased, compressed, password-protected, or encrypted files. Since ESI is
9 extremely vulnerable to inadvertent or intentional modification or destruction (both from
10 external sources and from destructive code embedded in the system such as a "booby
11 trap"), a controlled environment is often essential to ensure its complete and accurate
12 analysis.

13 b. Volume of Evidence: The volume of data stored on many digital
14 devices is typically so large that it is impossible to search for criminal evidence in a
15 reasonable period of time during the execution of the physical search of a search site. A
16 single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A
17 single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000
18 double-spaced pages of text. Computer hard drives are now being sold for personal
19 computers capable of storing up to four terabytes (4,000 gigabytes of data.) Additionally,
20 this data may be stored in a variety of formats or may be encrypted (several new
21 commercially available operating systems provide for automatic encryption of data upon
22 shutdown of the computer).

23 c. Search Techniques: Searching the ESI for the items described in
24 Attachment B may require a range of data analysis techniques. In some cases, it is
25 possible for agents and analysts to conduct carefully targeted searches that can locate
26 evidence without requiring a time-consuming manual search through unrelated materials
27 that may be commingled with criminal evidence. In other cases, however, such
28 techniques may not yield the evidence described in the warrant, and law enforcement

1 personnel with appropriate expertise may need to conduct more extensive searches, such
2 as scanning areas of the disk not allocated to listed files, or peruse every file briefly to
3 determine whether it falls within the scope of the warrant.

4 40. In this particular case, and in order to protect the third party privacy of
5 innocent individuals residing in the residence, the following are search techniques that
6 will be applied:

7 i. Device use and ownership will be determined through interviews, if
8 possible, and through the identification of user account(s), associated account names, and
9 logons associated with the device. Determination of whether a password is used to lock a
10 user's profile on the device(s) will assist in knowing who had access to the device or
11 whether the password prevented access.

12 ii. Use of hash value library searches.

13 iii. Use of keyword searches, i.e., utilizing key words that are known to be
14 associated with the sharing of child pornography.

15 iv. Identification of non-default programs that are commonly known to be used
16 for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent,
17 Ares, Shareaza, Gnutella, etc.

18 v. Looking for file names indicative of child pornography, such as, PTHC,
19 PTSC, Lolita, 3yo, etc. and file names identified during the undercover download of child
20 pornography.

21 vi. Viewing of image files and video files.

22 vii. As indicated above, the search will be limited to evidence of child
23 pornography and will not include looking for personal documents and files that are
24 unrelated to the crime.

25 41. These search techniques may not all be required or used in a particular
26 order for the identification of digital devices containing items set forth in Attachment B
27 to this Affidavit. However, these search techniques will be used systematically in an
28 effort to protect the privacy of third parties. Use of these tools will allow for the quick

1 identification of items authorized to be seized pursuant to Attachment B to this Affidavit,
2 and will also assist in the early exclusion of digital devices and/or files which do not fall
3 within the scope of items authorized to be seized pursuant to Attachment B to this
4 Affidavit.

5 42. In accordance with the information in this Affidavit, law enforcement
6 personnel will execute the search of digital devices seized pursuant to this warrant as
7 follows:

8 a. Upon securing the search site, the search team will conduct an initial
9 review of any digital devices/systems to determine whether the ESI contained therein can
10 be searched and/or duplicated on site in a reasonable amount of time and without
11 jeopardizing the ability to accurately preserve the data.

12 b. If, based on their training and experience, and the resources
13 available to them at the search site, the search team determines it is not practical to make
14 an on-site search, or to make an on-site copy of the ESI within a reasonable amount of
15 time and without jeopardizing the ability to accurately preserve the data, then the digital
16 devices will be seized and transported to an appropriate law enforcement laboratory for
17 review and to be forensically copied ("imaged"), as appropriate.

18 c. In order to examine the ESI in a forensically sound manner, law
19 enforcement personnel with appropriate expertise will produce a complete forensic
20 image, if possible and appropriate, of any digital device that is found to contain data or
21 items that fall within the scope of Attachment B of this Affidavit. In addition,
22 appropriately trained personnel may search for and attempt to recover deleted, hidden, or
23 encrypted data to determine whether the data fall within the list of items to be seized
24 pursuant to the warrant. In order to search fully for the items identified in the warrant,
25 law enforcement personnel, which may include investigative agents, may then examine
26 all of the data contained in the forensic image/s and/or on the digital devices to view their
27 precise contents and determine whether the data fall within the list of items to be seized
28 pursuant to the warrant.

1 d. The search techniques that will be used will be only those
2 methodologies, techniques and protocols as may reasonably be expected to find, identify,
3 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to
4 this Affidavit.

5 e. If, after conducting its examination, law enforcement personnel
6 determine that any digital device is an instrumentality of the criminal offenses referenced
7 above, the government may retain that device during the pendency of the case as
8 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
9 the chain of custody, and litigate the issue of forfeiture. If law enforcement determines
10 that a particular digital device was not an instrumentality of the offenses listed above, that
11 device shall be returned to the person from whom it was seized within sixty days of the
12 date of the warrant, unless the government seeks and obtains permission from the Court
13 for its retention.

14 43. In order to search for ESI that falls within the list of items to be seized
15 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and
16 search the following items (heretofore and hereinafter referred to as "digital devices"),
17 subject to the procedures set forth above:

18 a. Any digital device capable of being used to commit, further, or store
19 evidence of the offense(s) listed above;

20 b. Any digital device used to facilitate the transmission, creation,
21 display, encoding, or storage of data, including word processing equipment, modems,
22 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

23 c. Any magnetic, electronic, or optical storage device capable of
24 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
25 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
26 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

27 d. Any documentation, operating logs and reference manuals regarding
28 the operation of the digital device, or software;

1 e. Any applications, utility programs, compilers, interpreters, and other
2 software used to facilitate direct or indirect communication with the device hardware, or
3 ESI to be searched;

4 f. Any physical keys, encryption devices, dongles and similar physical
5 items that are necessary to gain access to the digital device, or ESI; and

6 g. Any passwords, password files, test keys, encryption codes or other
7 information necessary to access the digital device or ESI.

44. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) are located at the SUBJECT PREMISES or on the SUBJECT PERSON as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices found therein. As shown by the aforementioned facts, I believe that the SUBJECT PERSON may be actively seeking sexually explicit relationships with minors and actively attempting to manufacture child pornography. I therefore request that the court issue a warrant authorizing a search of the location, vehicles, and person specified in Attachment A for the items more fully described in Attachment B.

Subscribed and sworn to before me this 3rd day of January, 2020. In addition to the foregoing affidavit, I have also reviewed Exhibit 1 and upon completion of my review, placed the disc containing Images 1 and 2 back in the envelope, sealed the envelope, and affixed my signature across the sea.


J. RICHARD CREATURA
United States Magistrate Judge

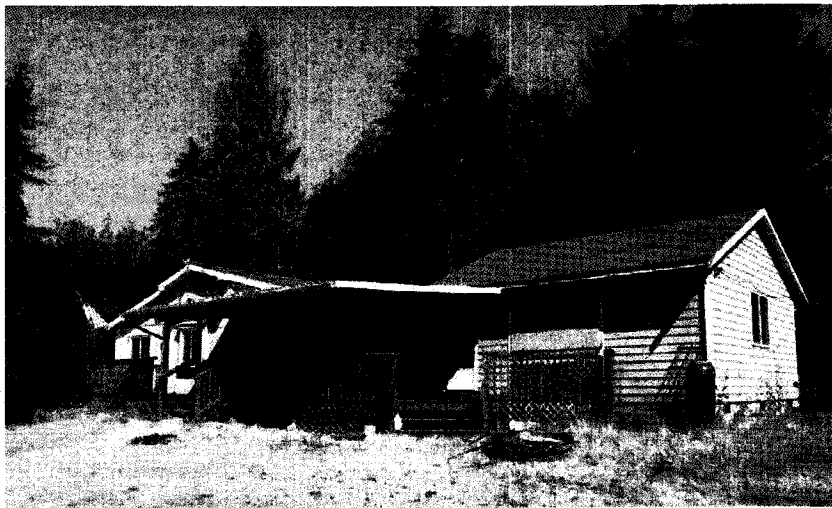
ATTACHMENT A

Description of Property to be Searched

1. The physical address of the SUBJECT PREMISES is 20205 117th Ave East, Graham, Washington 98338. The SUBJECT PREMISES is further described as the property containing a single family, single story residence located in Pierce County, WA.



Back

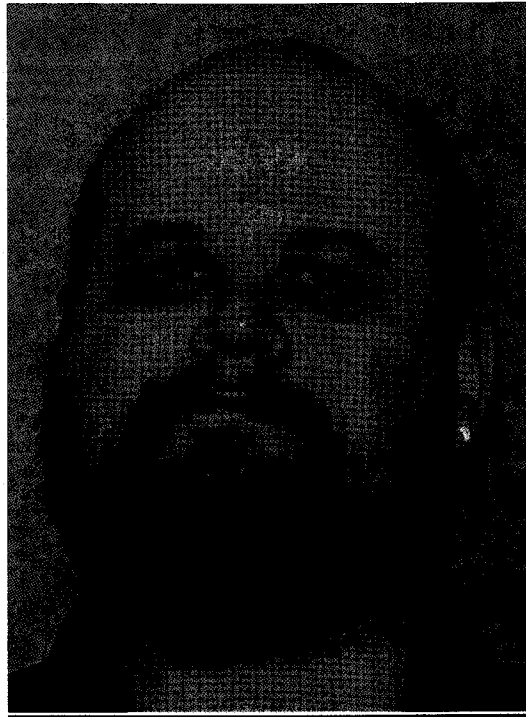


The search is to include all rooms and vehicles on the SUBJECT PREMISES, as well as any garage/parking spaces or storage units/outbuildings located thereon and any digital device(s) found therein. Specifically, this warrant authorizes law enforcement to

1 seize and search any digital device law enforcement has probable cause to believe is
2 owned by or to which the SUBJECT PERSON has access. ~~For any other digital device,~~
3 ~~law enforcement may seize that device under this warrant but may not search it without~~
4 ~~approval from the Court.~~

(M)
JRC

5
6 The SUBJECT PERSON is NATHANIEL MARCUS SCOTT (DOB:
7 XX/XX/1973), pictured below:



ATTACHMENT B**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES or on the SUBJECT PERSON:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media and any items depicted in those visual depictions that may help to identify the person depicted or the creator of the depictions;

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence/records identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer, or evidences contact with minors;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

1 a. Any digital devices and storage device capable of being used to
2 commit, further, or store evidence of the offense listed above;

3 b. Any digital devices used to facilitate the transmission, creation,
4 display, encoding or storage of data, including word processing equipment, modems,
5 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

6 c. Any magnetic, electronic, or optical storage device capable of
7 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
8 memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives,
9 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

10 d. Any documentation, operating logs and reference manuals regarding
11 the operation of the digital device or software;

12 e. Any applications, utility programs, compilers, interpreters, and other
13 software used to facilitate direct or indirect communication with the computer hardware,
14 storage devices, or data to be searched;

15 f. Any physical keys, encryption devices, dongles and similar physical
16 items that are necessary to gain access to the computer equipment, storage devices or
17 data; and

18 g. Any passwords, password files, test keys, encryption codes or other
19 information necessary to access the computer equipment, storage devices or data;

20 8. Evidence of who used, owned or controlled any seized digital device(s) at
21 the time the things described in this warrant were created, edited, or deleted, such as logs,
22 registry entries, saved user names and passwords, documents, and browsing history;

23 9. Evidence of malware that would allow others to control any seized digital
24 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
25 as evidence of the presence or absence of security software designed to detect malware;
26 as well as evidence of the lack of such malware;

27 10. Evidence of the attachment to the digital device(s) of other storage devices
28 or similar containers for electronic evidence;

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

12. Evidence of times the digital device(s) was used;

13. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

14. Records and things evidencing the use of the IP addresses 73.221.4.33 (the SUBJECT IP ADDRESS) including:

a. Routers, modems, and network equipment used to connect computers to the Internet;

b. Records of Internet Protocol (IP) addresses used;

c. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

SEARCH TECHNIQUES

1. In this particular case, and in order to protect the third party privacy of innocent individuals residing in the residence, the following are search techniques that will be applied:

i. Device use and ownership will be determined through interviews, if possible, and through the identification of user account(s), associated account names, and log-ons associated with the device. Determination of whether a password is used to lock a user's profile on the device(s) will assist in knowing who had access to the device or whether the password prevented access.

ii. Use of hash value library searches.

iii. Use of keyword searches, i.e., utilizing key words that are known to be associated with the sharing of child pornography.

iv. Identification of non-default programs that are commonly known to be used for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent, Ares, Shareaza, Gnutella, etc.

1 v. Looking for file names indicative of child pornography, such as, PTHC,
2 PTSC, Lolita, 3yo, etc. and file names identified during the undercover download of child
3 pornography.

4 vi. Viewing of image files and video files.

5 vii. As indicated above, the search will be limited to evidence of child
6 pornography and will not include looking for personal documents and files that are
7 unrelated to the crime.

8 2. These search techniques may not all be required or used in a particular
9 order for the identification of digital devices containing items set forth in Attachment B
10 to this Affidavit. However, these search techniques will be used systematically in an
11 effort to protect the privacy of third parties. Use of these tools will allow for the quick
12 identification of items authorized to be seized pursuant to Attachment B to this Affidavit,
13 and will also assist in the early exclusion of digital devices and/or files which do not fall
14 within the scope of items authorized to be seized pursuant to Attachment B to this
15 Affidavit.

16 3. In accordance with the information in this Affidavit, law enforcement
17 personnel will execute the search of digital devices seized pursuant to this warrant as
18 follows:

19 a. Upon securing the search site, the search team will conduct an initial
20 review of any digital devices/systems to determine whether the ESI contained therein can
21 be searched and/or duplicated on site in a reasonable amount of time and without
22 jeopardizing the ability to accurately preserve the data.

23 b. If, based on their training and experience, and the resources
24 available to them at the search site, the search team determines it is not practical to make
25 an on-site search, or to make an on-site copy of the ESI within a reasonable amount of
26 time and without jeopardizing the ability to accurately preserve the data, then the digital
27 devices will be seized and transported to an appropriate law enforcement laboratory for
28 review and to be forensically copied ("imaged"), as appropriate.

1 c. In order to examine the ESI in a forensically sound manner, law
2 enforcement personnel with appropriate expertise will produce a complete forensic
3 image, if possible and appropriate, of any digital device that is found to contain data or
4 items that fall within the scope of Attachment B of this Affidavit. In addition,
5 appropriately trained personnel may search for and attempt to recover deleted, hidden, or
6 encrypted data to determine whether the data fall within the list of items to be seized
7 pursuant to the warrant. In order to search fully for the items identified in the warrant,
8 law enforcement personnel, which may include investigative agents, may then examine
9 all of the data contained in the forensic image/s and/or on the digital devices to view their
10 precise contents and determine whether the data fall within the list of items to be seized
11 pursuant to the warrant.

12 d. The search techniques that will be used will be only those
13 methodologies, techniques and protocols as may reasonably be expected to find, identify,
14 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to
15 this Affidavit.

16 e. If, after conducting its examination, law enforcement personnel
17 determine that any digital device is an instrumentality of the criminal offenses referenced
18 above, the government may retain that device during the pendency of the case as
19 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
20 the chain of custody, and litigate the issue of forfeiture. If law enforcement determines
21 that a particular digital device was not an instrumentality of the offenses listed above, that
22 device shall be returned to the person from whom it was seized within sixty days of the
23 date of the warrant, unless the government seeks and obtains permission from the Court
24 for its retention.

25 4. In order to search for ESI that falls within the list of items to be seized
26 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and
27 search the following items (heretofore and hereinafter referred to as "digital devices"),
28 subject to the procedures set forth above:

1 a. Any digital device capable of being used to commit, further, or store
2 evidence of the offense(s) listed above;

3 b. Any digital device used to facilitate the transmission, creation,
4 display, encoding, or storage of data, including word processing equipment, modems,
5 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

6 c. Any magnetic, electronic, or optical storage device capable of
7 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
8 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
9 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

10 d. Any documentation, operating logs and reference manuals regarding
11 the operation of the digital device, or software;

12 e. Any applications, utility programs, compilers, interpreters, and other
13 software used to facilitate direct or indirect communication with the device hardware, or
14 ESI to be searched;

15 f. Any physical keys, encryption devices, dongles and similar physical
16 items that are necessary to gain access to the digital device, or ESI; and

17 g. Any passwords, password files, test keys, encryption codes or other
18 information necessary to access the digital device or ESI.

19 **The seizure of digital devices and/or their components as set forth herein is**
20 **specifically authorized by this search warrant, not only to the extent that such**
21 **digital devices constitute instrumentalities of the criminal activity described above,**
22 **but also for the purpose of the conducting off-site examinations of their contents for**
23 **evidence, instrumentalities, or fruits of the aforementioned crimes.**
24
25
26
27
28